REQUEST FOR PROPOSALS

ACQ-2013-0501-RFQQ

QUESTIONS & ANSWERS DOCUMENT

MAY 16, 2013

The Administrative Office of the Courts published the Request of Qualifications and Quotations, ACQ-2012-0501-RFQQ, on May 8, 2013 for the IT Security Review & Compliance Audit. As required under RFQQ Section 1.8 – Acquisition Schedule, answers to Vendor submitted questions are provided below.

Q1: In conducting the assessment what are the preferred security frameworks/standards your organization utilizes?

A1: AOC uses the Judicial Information System (JIS) IT Security Policy and Standards.

Q2: How many, what operating systems are in use, and where are they located (off-site, etc)?

A2: AOC has 3 operating systems: Z/OS, Windows, and Linux. They are located at the AOC data center and at four (4) other offsite locations.

Q3: Are there any specific tools prohibited by the organization for internal or external penetration testing?

A3: No.

Q4: a) Is there a standardized “corporate policy” utilized throughout the organization?
b) Are you seeking a policy and staff training review?
c) If so, do your off-site locations involved in this RFP have unique contingency plans/emergency plans, or are they the same (excluding geographic specific details)?

A 4: a) See A1 for a response.
b) Yes.
c) AOC off site locations have the same contingency plans/emergency plans.

Q5: Are breach reports available?

A5: Yes.

Q6: With regards to the assessment of network device configurations, is the focus to look at process platforms deployed and maintain or to look at each individual configuration specifically?

A6: AOC expects the selected Vendor to the focus review of process platforms deployed and maintained.

Q7: Is cloud computing utilized and is that part of the assessment?

A7: No.

Q8: Are third party vendors utilized and included in the assessment?

A8: No.

Q9: Is the IT network centralized or are there offsite locations? If so, how many and where are the site(s) location(s) and their geographical addresses/locations? If these locations are FOUO classified, please provide a focal point by address and/or approximate travel miles to location(s).

A9: AOC has a centralized IT network with a few servers at other offsite locations. This information will be provided to the selected Vendor following contract execution. N/A.

Q10: What is the total quantity of IP based devices per site and total for the organization?

A10: AOC, as a whole, has thousands of IP based devices used within its organization.

Q11: Are wireless systems part of the assessment? If so, are they IP addressable? Are they employed on a Single or Multiple System Network? Please describe in specificity the types, quantity of devices utilized and their "site" locations. If these locations are FOUO classified, please provide a focal point by address and/or approximate travel miles to location(s).

A11: Yes. No. They are employed on a Multiple System Network. AOC maintains 48 wireless devices at its main data center with an additional 40 devices at the other offsite locations. N/A.

Q12: Does the assessment include mobile devices? If so, how many? Are they IP addressable? Are they employed on a single or multiple System Network? If these locations are FOUO classified, please provide a focal point by address and/or approximate travel miles to location(s).

A12: No. N/A. No. N/A. N/A.

Q13: What are the total number of scans you would require conducted for both external and internal?

A13: AOC is relying on the Vendor's expertise to determine the necessary quantity.

Q14: Do you desire a representative scan or 100% of all devices?

A14: AOC is relying on the Vendor's expertise to determine the necessary quantity.

Q15: RFQQ Section 5.7 – Will we be given the number of IP address counts expected, both internal and external?

A15: Yes. Further clarification will be provided to the selected Vendor upon contract execution.

Q16: RFQQ Section 5.7 – Will we be provided a list of IP addresses or ranges to either stay within and/or avoid?

A16: No.

Q17: RFQQ Section 5.7 – For the IPT, will we be given the number of applications and approximate sizes/installation counts of those applications?

A17: Yes.

Q18: RFQQ Section 5.7 – For the IPT, after initial attempts from external sources would a device be allowed to be inserted into the network as a base for further testing?

A18: Yes

Q19: RFQQ Section 5.11 – What types of social engineering engagements are allowed and or preferred?
a) Email
b) Telephone
c) Onsite (please provide number of locations)

A19: In response to a) and b) in Q19, please refer to ATTACHMENT A – Statement of Work, Task 6 within EXHIBIT C – Draft Contract. In response to c) in Q19, AOC expects the Vendor to provide onsite social engineering engagements at 3 locations.

Q20: RFQQ Section 5.11 – Are these engagement types at the vendor discretion?

A20: Yes.

Q21: RFQQ Section 5.11 – Are there any types of engagements that would not be allowed?

A21: Yes. Further clarification will be provided to the selected Vendor upon contract execution.

Q22: RFQQ Section 5.7.1 – It's understood that AOC would like the Vendor to conduct Digital Footprinting to identify publicly available information that would support in initiating an attack. Will AOC at any point also provide the Vendor with the full IP ranges and URL's through which to attempt to exploitation, or, will that all be reliant on what the Vendor identifies?

A22: See A15 for a response.

Q23: RFQQ Section 5.7.1 – Approximately how many IP addresses does AOC have that are Internet facing?

A23: AOC has one (1) class C address that is internet facing.

Q24: RFQQ Section 5.7.1 – Can testing be performed during business hours?

A24: Yes

Q25: RFQQ Section 5.7.1 – How many websites and web applications are in-scope?

A25: All AOC websites and web applications shall be considered in scope.

Q26: RFQQ Section 5.7.1 – Is AOC looking for a network penetration test for all public-facing systems and network devices or a sample of these?

A26: AOC looking for a network penetration test for ***all*** public-facing systems and network devices

Q27: RFQQ Section 5.7.1 – For each in-scope website and web application, how many users use the application?

A27: Users count varies between each in-scope website and web application.

Q28: RFQQ Section 5.7.1 – For each in-scope website and web application, how many users use the application at each level of credentials & what is each role?

A28: User count per credential level varies between the in-scope websites and web applications.

Q29: RFQQ Section 5.7.1 – For each in-scope website and web application, if you had to characterize the code base & architecture, would you say its small and simple or a large and complex application?

A29: AOC would characterize the code base and architecture of the various websites and web applications as large and complex.

Q30: RFQQ Section 5.7.1 – For each in-scope website and web application, is the application browser based, or client-server?

A30: All AOC websites and web applications are browser based.

Q31: RFQQ Section 5.7.1 – For each in-scope website and web application, is the application web-facing (accessible directly from the Internet) or does it require VPN/Citrix/RDP to access remotely?

A31: In-scope websites and web applications are a mixture of both web-facing and VPN/Citrix/RDP remote accessible.

Q32: RFQQ Section 5.7.1 – For each in-scope website and web application, what are the hosting platforms (i.e., Linux or MS over Apache, IIS over 2003, etc.)?

A32: Hosting platforms operate under the following application server architectures: Websphere, IIS, BizTalk and Apache .

Q33: RFQQ Section 5.7.1 – For each in-scope website and web application, what language or framework has the application been developed in (e.g., PHP, ASP, JSP, .NET, ColdFusion, etc.)?

A33: Language or framework operates under the following: uniPaaS, Java, Coldfusion, and .NET.

Q34: RFQQ Section 5.7.1 – For each in-scope website and web application, is the application to be assessed in a production or test environment?

A34: AOC is not placing a limit on the scope specifically related to the External Penetration Testing and Assessment.

Q35: RFQQ Section 5.7.1 – For each in-scope website and web application, is the application internally developed or Custom of the Shelf (COTS)?

A35: Currently, AOC applications are only developed internally.

Q36: RFQQ Section 5.7.1 – For each in-scope website and web application, will login credentials be provided for the assessment? If so, how many levels need to be assessed (Admin, employee, self-registered customer)?

A36: Yes. Up to 5 different levels will need to be assessed by the Vendor.

Q37: RFQQ Section 5.7.1 – For each in-scope website and web application, approximately how many pages does each web application in scope contain?

A37: Cumulatively, AOC websites contain approximately a hundred thousand (100,000) webpages.

Q38: RFQQ Section 5.7.1 – Are all public-facing systems centrally managed?

A38: Yes.

Q39: RFQQ Section 5.7.2 – It's understood Vendor will be provided little information. Will Vendor be provided with basic-user level credentials to access the environment?

A39: Yes.

Q40: RFQQ Section 5.7.2 – Approximately how many active internal IPs does AOC have that in-scope?

A40: AOC currently has 12 Class C active IP addresses.

Q41: RFQQ Section 5.7.2 – How many internal network segments?

A41: AOC has no more than 25 internal network segments

Q42: RFQQ Section 5.7.2 – Can access be provided such that the assessor could reach all in-scope systems from a single network location?

A42: Yes

Q43: RFQQ Section 5.7.2 – Can internal testing be performed remotely via VPN, or is it preferred that testing take place onsite? If onsite, please provide the address for each location.

A43: Some testing will be required to be completed onsite. This type of testing will be completed onsite at AOC in Olympia, WA.

Q44: RFQQ Sections 5.8 and 5.11 – It's understood AOC would like Vendor to perform Social Engineering to validate the physical security controls and employee awareness training program are operating effectively. Please provide the address for each location in-scope for attempting to gain physical access.

A44: Locations for physical access for Social Engineering will occur at Olympia and Sea-Tac, WA.

Q45: RFQQ Sections 5.8 and 5.11 – Are there any specific types of social engineering (phishing, physical social engineering, pretext calling, etc) the agency is interested in conducting?

A45: See A19 for a response.

Q46: RFQQ Sections 5.8 and 5.11 – What is the variety and quantity of operating systems included in the scope of the assessment?

A46: See A2 for a response.

Q47: RFQQ Sections 5.8 and 5.11 – How many systems are included in total?

A47: See A2 for a response.

Q48: RFQQ Sections 5.8 and 5.11 – Is data encrypted in databases or flat files?

A48: AOC has both encrypted and non-encrypted.

Q49: RFQQ Sections 5.8 and 5.11 – How many types of encryption are in use?

A49: AOC uses industry standard encryption. Details will be revealed to the selected Vendor following contract execution.

Q50: RFQQ Sections 5.8 and 5.11 – How many different database platforms will be included in the scope of the applications?

A50: Two (2) different database platforms are considered in scope of the applications.

Q51: RFQQ Sections 5.8 and 5.11 – Will the assessment include the 58+ supported applications noted in the RFQQ?

A51: Yes.

Q52: RFQQ Sections 5.8 and 5.11 – How many personnel are involved in the management of the systems and applications in scope for the assessment?

A52: Over 120 personnel are involved in the systems and applications in scope for the assessment.

Q53: RFQQ Sections 5.8 and 5.11 – How many departments and application owners (that manage approval and access to systems) are included in the scope of the assessment?

A53: Up to 12 departments and application owners are included in the scope of the assessment.

Q54: RFQQ Sections 5.8 and 5.11 – What is the overall network architecture for protecting systems (Checkpoint front end, DMZ, MPLS for remote location connectivity, etc)?

A54: AOC's Overall network architecture for protecting systems includes F5 SSL appliance, DMZ, Checkpoint and VPN appliance.

Q55: RFQQ Sections 5.8 and 5.11 – How many firewalls are in use? Is the configuration of the firewalls similar? Can the review be conducted on a sample of firewalls instead of all firewalls? All 4 primary firewalls will be required to be reviewed.

A55: AOC maintains eight (8) firewalls. No. All four (4) primary firewalls will be required to be reviewed by Vendor.

Q56: RFQQ Sections 5.8 and 5.11 – How many types of anti-virus deployments are in use across the agency? Are they centrally managed?

A56: AOC maintains 4 different types of anit-virus deployments across the agency. These deployments are centrally managed.

Q57: RFQQ Sections 5.8 and 5.11 – Does the review of 'user account administration practices and procedures' include a review of the Active Directory deployment or a review of group policies and configurations?

A57: The review of 'user account administration practices and procedures' shall include ***both*** the Active Directory deployment and a review of group policies and configurations.

Q58: RFQQ Sections 5.8 and 5.11 – The RFQQ requests a risk analysis/testing of 'Validate separation of suited and dual control issues'. Please provide more information regarding what security controls/ areas the agency is looking to cover?

A58: Further clarification shall be provided to the selected Vendor upon contract execution.

Q59: RFQQ Sections 5.9 – Please confirm, as stated, that the Control Design Review is limited to application controls.

A59: The Control Design Review deliverable will not be limited solely to application controls.

Q60: RFQQ Sections 5.9 – How many physical locations are included in the scope of the assessment for: 1) Data Centers? 2) Court/site locations?

A60: Please refer to second response provided in A2 for a response to both questions.

Q61: RFQQ Sections 5.9 – Are the systems a subset of the systems included in the Vulnerability Assessment? If not, what is the variety and quantity of operating systems included in the scope of the assessment? How many systems are included in total?

A61: Yes. N/A. N/A.

Q62: RFQQ Sections 5.9 – How many of the 58+ applications will be included in the scope of the assessment?

A62: All of the 58+ applications will be included in the scope of the assessment.

Q63: RFQQ Sections 5.9 – How many locations will be included in the scope? Are all locations in Olympia?

A63: All locations will be included in the scope. Not all locations are in the local vicinity of Olympia, WA.

Q64: RFQQ Sections 5.9 – How many individuals are anticipated to be included in the analysis?

A64: All access levels of AOC employees and contracted staff must be considered for these evaluations.

Q65: RFQQ Sections 5.9 – Are basic processes and procedures formally documented?

A65: Yes.

Q66: RFQQ Sections 5.9 – Are the systems for each of the business units identified centrally managed by the business unit?

A66: Yes

Q67: RFQQ Sections 5.10 – Is the scope of the Security Plan the same as the Vulnerability Assessment? If not, explain the scope of the Security Plan. What are the expectation for documenting and maintaining the security plan (format, online repositories, etc)?

A67: No, the scope for the Security Plan is not the same as the scope for the Vulnerability Assessment. AOC expects the results of the audit and penetration tests to be used to develop a revised security plan for AOC. AOC expects the Vendor to use industry standards (i.e., NIST, SANS) for documenting and maintaining the security plan.

Q68: RFQQ Sections 5.10 – Will all communication tools and repositories be developed and maintained by AOC?

A68: Yes.

Q69: RFQQ Sections 5.10 – How many departments will be included in the Security Plan process?

A69: Refer to A53 for a response.

Q70: RFQQ Sections 5.10 – Is there an expectation, under this contract, that the vendor will help implement the security plan or just assess and recommend the plan based on the analysis?

A70: The expectation as set forth under this RFQQ is for the awarded Vendor to assess and recommend the plan based on the analysis.

Q71: RFQQ Sections 5.10 – How many locations will be included in the scope? Are all locations in Olympia?

A71: Refer to the second response provided under A2.

Q72: RFQQ Sections 5.10 – How many individuals are anticipated to be included in the analysis?

A72: Refer to A52 for a response.

Q73: RFQQ Sections 5.10 – Please advise as to any legal or regulatory compliance related obligations that AOC is aware of (i.e., PCI, State Data Privacy, CJIS, FISMA, etc.).

A73: Refer to Sections 30 and 31 of EXHIBIT C – Draft Contract for more information.

Q74: RPQQ Section 4.3.3 – Please clarify this section which states "AOC requires, at a minimum, each key project staff proposed by Vendor to hold current IT professional security certification with designations of Certified INFORMATION Systems Security Professional (CISSP)." Staffing for a project may require project managers or staff focused on a particular specialty. Is the CISSP a requirement in addition to the targeted certifications required to perform the Security Review for all staff? Can some staff members have specific certifications that security related but not have the CISSP?

A74: At a minimum, the Technical Security Lead as a key project staff member must have a current CISSP certification. Yes, other Vendor project staff is encouraged to have current security related certifications specific to their position as identified in the Vendor's proposed organization chart for their project team. Vendor will be required to show proof of certifications upon contract award of all certifications noted in the proposal for project staff. Vendor will be required to maintain compliance to such staff certifications throughout the term of any executed contract.

Q75: RFQQ Section 4.3.3 – Please clarify this section which states "At a minimum, proposed Technical Security Lead must have a U.S. National Security Clearance of the appropriate level." Is a US National Security Clearance a mandatory requirement for the Tech Lead and what would be the appropriate level? As there can be a significant time interval to process background checks are interim security clearances sufficient?

A75: Yes, the Technical Security lead is required to have a US National Security Clearance. The security clearance must be at the Federal Secret level. AOC highly prefers a fully vetted security clearance at this required level. However, interim security clearances will be acceptable for the first 6 months of any contract awarded as a result of this RFQQ. Vendor will be required to show proof of compliance to this requirement for US National Security clearances upon contract award. Vendor will be required to maintain compliance to such staff certifications throughout the term of any executed contract.

Q76: RFQQ Section 5.6 – Approximately how many pages are included in AOC's Security Policy and Practices documentation?

A76: Approximately 55 pages are included in AOC's Security Policy and Practices documentation.

Q77: RFQQ Section 5.6 – Approximately how many policies are included in the Security Policy and Practices documentation?

A77: Approximately fifty (50) policies are included in AOC's Security Policy and Practices documentation.

Q78: RFQQ Section 5.6 – Approximately how many policies are included in the 'Data Dissemination', 'Data Classification' and 'Handling of Sensitive Documents and Information' documentation?

A78: Less than ten (10) policies are included in the 'Data Dissemination', 'Data Classification' and 'Handling of Sensitive Documents and Information' documentation.

Q79: RFQQ Section 5.6 – Are the policies and practice documentation maintained by single, centralized group or are they decentralized?

A79: Maintenance for AOC's Security Policy and Practices documentation is decentralized.

Q80: RFQQ Section 5.6 – What are the high level topics covered in AOC's Security Policy and Practices?

A80: AOC's Security Policy and Practices includes the following high level topics:

1) Class: Management
   a) Risk Assessment
   b) Security Planning
   c) System and Services Acquisition
   d) Security Control Review
   e) Processing Authorization
2) Class: Operational
   a) Personnel Security
   b) Physical and Environmental Security
   c) Contingency Planning
   d) Configuration Management
   e) Hardware and Software Maintenance
   f) System and Information Integrity
   g) Media Protection
   h) Incident Responses
   i) Security Awareness and Training
3) Class: Technical
   a) Identification and Authentication
   b) Logical Access Control
   c) Accountability (including Audit Trails)
   d) System and Communications Protection

Q81: RFQQ Section 5.6 – Do "Practices" include processes, procedures, standards or is there another definition or type of practice that falls under this category?

A81: Yes, “Practices” include processes, procedures, and standards.

Q82: RFQQ Section 5.6 – Is the AOC’s current Security Policy and Practices documentation intended to align with any legal and/or regulatory compliance requirements? If so, which ones?

A82: Yes. AOC’s current Security Policy and Practices documentation was developed in alignment with National Institute of Standards and Technology (NIST) Special Publication 800-30 *Risk Management Guide for Information Technology Systems* (Jan. 2002) and NIST Special Publication 800-53 *Recommended Security Controls for Federal Information Systems* (Oct. 2003 draft).

Q83: What is the estimate of IP addresses under management and in scope of this contract?

A83: 13 class C IP addresses are under AOC management and shall be considered in scope of any contract resulting from this RFQQ.

Q84: RFQQ Section 4.3.3 states “At minimum, proposed Security Technical Lead must have a US National Security Clearance of the appropriate level”. What is the appropriate level? Does the Security Clearance need to be active at time of the proposal or at contract start?

A84: See A75 for response.

Q85: Is it possible to get us word version ASAP of the following documents: 1) ACQ-2013-0501-RFQQ.pdf, 2) EXHIBIT C - Draft Contract.pdf and 3) EXHIBIT D - Exceptions to Contract.pdf? The purpose of these documents being in WORD format is to make sure we accurately copy any exceptions from the draft contract and RFQQ document to incorporate in the Exceptions document.

A85: The RFQQ document, ACQ-2013-0501-RFQQ, will not be made available in WORD format. However, EXHIBITS C and D can are now available in WORD format at www.courts.wa.gov\procure.

Q86: During the project will the vendor be provided with the valuation of assets so that reasonable safeguards can be recommended according to asset value? Or, will the vendor assess the value of assets as part of this effort?

A86: AOC cannot provide a response without a clear definition of “assets”.

Q87: Will the vendor be provided with historical data, prior risk analysis, internal compliance audits, or other sources of prior evaluative information?

A87: Yes.

Q88: Is a staged staffing project approach that utilizes different skills during each project stage allowable, so that staff is brought on to the project only when their expertise is needed? Or, is a constant team configuration required for the duration of the project?

A88: Yes. No.

Q89: IP counts for external?

A89: Refer to A23 for a response.

Q90: IP counts for internal?

A90: Refer to A40 for a response.

Q91: # of apps for IPT? Approximate sizes?

A91: Refer to A62 for a response. Applications are in various sizes.

Q92: Will you allow RNA?

A92: Passive monitoring is acceptable. Vendor shall be responsible for not impacting AOC business functions.

Q93: What types of social engineering? if onsite, # of locations?

A93: Refer to A2 for a response.

Q94: How many internet-facing sites (IPs/domains) are in scope for external penetration test?

A94: AOC has 1 Class C IP address and 2 domains which shall be considered in scope for external penetrations tests.

Q95: How many internet-facing applications are in scope? How many multiple apps can be run on the same domain?

A95: Refer to A 62 for a response. AOC operates 2 public internet domains.

Q96: How many IPs (clients/servers) are in scope for internal penetration test?

A96: Refer to A 40 for a response.

Q97: The Technical Security Lead needs to have a National Security Clearance of an appropriate level, what level is that?

A97: See A75 for a response.

Q98: Do any of the other people need to have a National Security Clearance? If so, what level?

A98: See A75 for a response.

Q99: To ensure appropriate skill sets are identified: 1) Vendor hardware and software version of mainframe(s) in scope? 2) Number and descriptions of mainframe applications in scope?

A99: 1) IBM 2098 z/OS 1.11, 2) Refer to http://www.courts.wa.gov/jis/.

Q100: Please provide a listing of the number of physical locations in which you support your IT infrastructure?

A100: AOC has a total of seven (7) physical location in which AOC provides IT infrastructure support.

Q101: What outcome is expected, if any, other than a written report with gaps and recommendations?

A101: Refer to ATTACHMENT A – Statement of Work for further information.

Q102: Is there more than one set of policies and procedures?

A102: Refer to A77 for a response.

Q103: Is there a preferred Risk evaluation approach that you would like to use for the Risk Analysis and Control testing?
a) NIST
b) ISO 27001/27002
c) Other – Please elaborate.

A103: Refer to A67 for a response.

Q104: Are there any internal security standards that devices, systems, processes or applications should be compared against for the report?

A104: Yes.

Q105: What is the total number IP Addresses/hosts (Internet Accessible) that will be in scope for the assessment? For example: a) 15 hosts, b) 3 class C network segments

A105: Refer to A23 for a response.

Q106: How many of these services are web sites (HTTP and HTTPS)?

A106: AOC cannot provide a response without additional information regarding context.

Q107: Are any of the web services hosted at a third party? If yes, how many?

A107: AOC cannot provide a response without additional information regarding context.

Q108: Is both authenticated and un-authenticated (anonymous) web application testing requested?
a) Authenticated testing will allow Vendor to determine if a user who has valid credentials can access restricted areas of the application or other user data.
b) Anonymous testing will only allow Vendor to identify issues from an attacker's perspective in which valid credentials have not been provided.

A108: Yes, Vendor will be required to provide both authenticated and un-authenticated web application testing.

Q109: Are you looking for onsite social engineering (impersonation), if so, how many locations?

A109: See A19 for a response.

Q110: Are you looking for off-site social engineering (telephone calls/ email phishing), or both?
a) How many targets and ploys do you wish to have in scope?

A110: See A19 for a response.

Q111: How many total servers (physical & virtual) are within the environment?

A111: 60 servers are within the environment.

Q112: How many workstations are used within the company?

A112: 250 workstations are used within AOC.

Q113: Would off-site network reconnaissance be agreeable in order to reduce costs? This would involve Vendor shipping a device with network scanning tools configured so that we may conduct the initial network discovery portion of the assessment remotely over a secure connection. The remainder of the assessment would involve on-site Vendor team members.

A113: No, offsite network reconnaissance would not be agreeable to AOC at this time.

Q114: Do you utilize Cloud Computing? If so, what services?
a) IaaS
b) PaaS
c) SaaS

A114: No. N/A.

Q115: Subsection 3.1.1, the second bullet point requests an email address for the facility from which Vendor would operate. Please advise if the vendor's web address is sufficient or if the vendor should provide the email address and telephone/fax number for the lead point of contact.

A115: See Amendment 1 for further information.

Any modifications to the RFQQ required as a result to answers provided by AOC will be provided as an amendment to the RFQQ. Any such amendment will be published as a separate RFQQ document and will be available at www.courts.wa.gov/procure/.

STATE OF WASHINGTON
1206 QUINCE ST SE ● P.O. Box 41170 ● Olympia, WA 98504-1170
360-753-3365 ● 360-586-8869 Fax ● www.courts.wa.gov